REMARKS

Claims 1-36 are pending. Claims 1, 6, 8, 9, 10, 16, 19, 20, 26, and 29 have been amended. No claims have been canceled or added. In view of the following remarks/arguments, withdrawal of all outstanding objections and rejections to the pending claims is respectfully requested.

Claim Objections

Claims 8, 10, and 20 are informally objected to because of informalities. More particularly, the Action indicates that claims 8, 10, and 20 refer to the "selection of the particular threat" of claims seven, and 17, but respectively depend on claims 5, 1, and 11. Claims 8, 10, and 20 have been amended to correct these claim language informalities.

Accordingly, withdrawal of the objections to claims 8, 10, and 20 is respectfully requested.

35 USC §101 Rejections

Claims 1-10 stand rejected under 35 USC §101 as being directed to non-statutory subject matter. More particularly, that Action asserts that the language of the claims raise a question as to whether the claims are directed merely to a method that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 USC §101. Applicant respectfully disagrees. Claim 1 as originally submitted recites "in a computer system, a method", which clearly points out in distinctly claims a embodied in

statutory subject matter. With respect to utility, it is respectfully submitted that claimed subject matter meets at least one stated objective, and thereby clearly shows utility.

Even in view of the original claim's recitation of statutory subject matter and utility, **claim 1** has been amended without prejudice to more particularly point out that the operations of the claimed method are "computer-implemented". More particularly, claim 1 was amended as follows: "~~In a computer system, a method for providing~~ A computer-implemented method for a computer-program module to provide application security threat-modeling". In view of this amendment, withdrawal of the 35 USC §101 rejections of claim 1 is respectfully requested.

As an additional matter, Applicant respectfully submits that this amendment to claim 1 does not necessitate new search or new grounds of rejection. This is because claim 1 as originally submitted recited "In a computer system, a method". Moreover, other claims pending in this application, claims with non-amended preambles, were already directed to devices with computer-executable instructions "for providing application security threat-modeling". For example, claim 21 recites" "A device comprising: a memory comprising computer-executable instructions for providing application security threat-modeling", and "a processor that is operatively coupled to the memory, the processor being configured to fetch and execute the computer-executable instructions from the memory, the computer-executable instructions comprising instructions for [...]"

Accordingly, the amendments to the preamble of claim 1 correspond to subject matter that the Office has already had the opportunity to examine, and do

not necessitate new search or new grounds of rejection because of these amendments.

Claims 2-10 depend from claim 1. Thus, "[a] method as recited in claim 1", as indicated by respective ones of claims 2-7, and "[a] method as recited in claim 7" (claim 7 depends from claim 1), as indicated by respective ones of claims 8-10, refer to the "computer-implemented method" of claim 1.

Accordingly, withdrawal of the 35 USC §101 rejections of claims 2-10 is respectfully requested.

35 USC §112, Second Paragraph, Rejections

Claims 6, 9, 16, 19, 26, and 29 stand rejected under 35 USC §112, second paragraph, as failing to perfectly point out and distinctly claim subject matter regarded as the invention.

Claims 9, 19, and 29 have been amended to change the phrase "a desired level of strength technology" to "a desired level of strength of technology". In view of these amendments, withdrawal of the 35 USC §112, second paragraph, rejections of claims of 9, 19, and 29 is respectfully requested.

Claims 6, 16, and 26 have been amended to change the phrase "addressed security threats" to "a particular security threat similar to a security threat already addressed with respect to the particular component". These claim amendments provide appropriate antecedent basis for this feature of claims 6, 16, and 26. In view of these amendments, withdrawal of the 35 USC §112, second paragraph, rejections of claims 6, 16, and 26 is respectfully requested.

Claim Rejections Under 35 USC §102(a)

Claims 1-36 stand rejected under 35 USC §102(a) as being anticipated by "Security Analysis & Design" by Uttara Nerurkar ("Nerurkar"). This rejection is traversed.

Claim 1 recites "[a] computer-implemented method for a computer-program module to provide application security threat-modeling, the method comprising: defining a plurality of model components to represent respective elements of an application, each model component comprising a respective set of potential security threats", "interconnecting the model components to form a logical model of the application", and "analyzing one or more of the potential security threats in terms of the model components in the logical model."

In addressing claim 1, the Action (page 4) asserts that Nerurkar describes these recited features at page 50, column 3, ¶ 4; page 50, column 2, ¶ 2; page 52, column 1, ¶ 1; page 52, column 1, ¶ 3; and page 54, column 1, ¶3. Applicant respectfully disagrees. Claim 1 recites "[a] computer-implemented method [...]" that sets forth multiple operations "to provide application security threat-modeling". Thus, the preamble "[a] computer-implemented method", by necessary implication, is given the effect of a limitation, because it provides life, meaning, and vitality to the recited operations in the claims. These cited portions of Nerurkar, and Nerurkar as a whole, are completely silent (i.e., do not explicitly or inherently describe) "[a] computer-implemented method" of any type. In fact, Nerurkar does not explicitly describe use of a computer to implement any portion of the security analysis and design described in the corresponding reference. Moreover, Applicant respectfully submits that nowhere does Nerurkar clearly

disclose the use of a computer to implement any portion of the security analysis and design described by Nerurkar is necessarily present.

For instance, Nerurkar at page 50, column 2, ¶s 1 and 2, merely describes the following: "**I put together** a security analysis and design/modeling technique that closely couples a security and functional model of the product. [...] the method broadly involves the following steps: 1. Determine the scope of the problem; that is, the product and its environment. 2. Partition this into zones having similar security concerns. 3. Analyze each zone for vulnerabilities in a structured way by focusing on the different stages in the access and use of objects in the zone 4. Design countermeasures for each vulnerability and choose one or more of them based on a coverage and cost."

Nerurkar, in the 2nd paragraph of the section titled "The Onion Peel Model" (50, column 3, ¶ 4), begins describing these steps of the method described in the preceding paragraph: "the model begins with a context diagram depicting the system and its environment. The difference here is that **I include** the nonphysical components of the environment in the model [...]". (Emphasis added). Beginning at page 52, ¶ 4, Nerurkar describes the following: "**I define** an Internet User Interface Peel consisting of the web interface of the application [...] the network components, on the other hand, are placed in the Internet Communications Peel [...] to illustrate further, an e-commerce web site may need to secure its interaction with the payment system much more than its interface with the online customer. In that case, **you should divide** the mentioned Internet User Interface Peel into the Customer Interface Peel and the Payment System Interface Peel." (Emphasis added; please also see page 52, col. 1, ¶'s 1-3, and page 54, col. 1, ¶ 3). Nerurkar continues at page 56, column 2, ¶ 2, wherein Nerurkar describes "[u]sing the

aforementioned LOP technique, **you can systematically analyze** the onion, its peels, and the object sets one by one, and design countermeasures **for the exposures you discover**. [...] **[I]f you find** that the controls run across peels or pure object sets, **you probably need to review** the peel projects at definition." (Emphasis added). In the last paragraph of column 2, page 56, Nerurkar also describes: "As a final step, go over the completed model once more to combine, separate, or remove security controls across LOPs, object sets, and peels. Take their coverage and cost into account."

In view of the above, it is clear that Nerurkar describes a system for security analysis and design that is to be implemented step-by-step by a human being, not by a computer. Applicant respectfully submits that Nerurkar does not even describe an option to implement the system of Nerurkar in a computer. Since Nerurkar does not identically disclose the claimed "computer-implemented method", which provides life, meaning, and vitality to the claimed operations of "defining a plurality of model components", "interconnecting", and "analyzing", Nerurkar does not anticipate these recited features of claim 1.

In view of the above, the Action has failed to present a prima facie case of anticipation of claim 1. Accordingly, withdrawal of the 35 USC §102(a) rejection of claim 1 is respectfully requested.

Claims 2-10 depend from claim 1 and are not anticipated by Nerurkar solely by virtue of this dependency. Accordingly, withdrawal of the 35 USC §102(a) rejections of claims 2-10 is respectfully requested.

Additionally, claims 2-10 include additional features that are not explicitly or inherently described by Nerurkar. For example, claim 2 recites "wherein the model components comprise a module, a port, a store, or a wire." In addressing

these features, the Action asserts that they are taught by Nerurkar's "network cabling" at page 50, column 3, ¶ 4. Applicant respectfully disagrees.

The recited "a module, a port, a store, or a wire" are for interconnecting "to form a logical model of an application", as claimed. The specification, at page 7, line 18, clearly discloses that a logical entity representing some portion of an application "has no physical manifestation." In contrast to these properties of a "a module, a port, a store, or a wire", Nerurkar explicitly describes in ¶ 4, the network cabling as a physical manifestation because it is any "known physical components of the environment. More particularly, Nerurkar explicitly describes that "known physical components of the environment [...] could include software components such as web servers, application servers, databases, and the like; and hardware components such as network cabling, satellite uplinks, and so on." Thus Nerurkar's explicit description at page 50, column 3, ¶ 4 does not explicitly or inherently describe the properties of "a module, a port, a store, or a wire", as recited in claim 2. In view of this, Nerurkar does not anticipate these claimed features.

Accordingly, and for these additional reasons, the 35 USC §102(a) rejection of claim 2 should be withdrawn.

In another example, claim 3 recites: "wherein the potential security threats comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation." In addressing these claimed features, the Action asserts that they are described by Nerurkar at page 56, column 1, ¶ 3. Applicant respectfully disagrees because this cited portion of Nerurkar is completely silent on any type of "non-repudiation", as claim 3 recites. The specification at page 6, lines 15-17, clearly describes "non-repudiation". More

particularly: "The non-repudiation security category is directed to providing proof that a particular action occurred so as to prevent a principal from denying the occurrence of the particular action." Nowhere does Nerurkar explicitly or inherently describe such "non-repudiation", as claim 3 recites.

Accordingly, and for this additional reason, the 35 USC §102(a) rejection of claim 3 should be withdrawn.

In another example, claim 5 recites "selecting a particular component of the model components", and "responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar potential security threats as the particular component." In addressing this claimed feature, the Action asserts that it is described by Nerurkar's partition based on the similarity and nature of security concerns of the components (page 52, column 1, ¶ 3). Applicant respectfully disagrees. A fundamental aspect of 35 USC §102(a) is that a claim is anticipated only if each and every element as set forth in the claim is described in a single prior art reference (MPEP §2131.01).

Nerurkar at page 52, column 1, ¶ 3, does not describe each and every element as set forth in claim 5. Instead, Nerurkar merely describes that "[t]he onion is now partitioned into peels based on the similarity in the nature and criticality of the security concerns of the components. [...] the peels are documented in the Peel Diagram." (Athough Nerurkar does explicitly show any diagram labeled "Peel Diagram", Applicant respectfully submits that this diagram is likely figure 1 of Nerurkar, which shows Peels in a financial product along with physical components thereof). Clearly, this teaching of Nerurkar is directed to indicating that a user partitions an onion into peels based on the indicated criteria.

Nowhere does this description teach that anything is done "responsive to selecting the particular component". Thus a system of Nerurkar may never "selecting a particular component of the model components", and "responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar potential security threats as the particular component", as claim 5 recites.

Accordingly, and for these additional reasons, the 35 USC §102(a) rejection of claim 5 should be withdrawn.

In another example, claim 6 recites "selecting a particular component of the model components", and "responsive to selecting the particular component, displaying each other component of the model components that comprises a particular security threat similar to a security threat already addressed with respect to the particular component." In addressing this claimed feature, the Action asserts that it is described by Nerurkar's at page 52, column 2, ¶ 4). Applicant respectfully disagrees.

Nerurkar at page 52, column 2, ¶ 4, merely defines an Internet User Interface Peel and describes placing network components in the Internet Communications Peel. The following paragraph of Nerurkar merely describes that because of interaction of an e-commerce application with a payment system, the Internet User Interface Peel should be divided into the Customer Interface Peel and Payment System Interface Peel. Clearly, nowhere do these explicit descriptions of Nerurkar teach that anything is done "responsive to selecting a particular component". If Nerurkar does not teach a claimed feature, Nerurkar cannot anticipate the claimed feature. Thus a system of Nerurkar may never "selecting a particular component of the model components", and "responsive to

selecting the particular component, displaying each other component of the model components that comprises a particular security threat similar to a security threat already addressed with respect to the particular component", as claim 6 recites.

Accordingly, and for these additional reasons, the 35 USC §102(a) rejection of claim 6 should be withdrawn.

Claim 11 recites: "A computer-readable medium comprising computer-executable instructions for providing application security threat-modeling, the computer-executable instructions comprising instructions for: defining a plurality of model components to represent respective elements of an application, each model component comprising a respective set of potential security threats", "interconnecting the model components to form a logical model of the application", and "analyzing one or more of the potential security threats in terms of the model components in the logical model." In addressing these claimed features, the Action rejects them on the same rationale used to reject claim 1. Applicant respectfully submits that for the same reasons discussed above with respect claim 1, Nerurkar does not anticipate claim 11.

Accordingly, withdrawal of the 35 USC §102(a) rejection of claim 11 is respectfully requested.

Claims 12-20 depend from claim 11 and are not anticipated by Nerurkar solely in view of these respective dependencies. For this reason alone, withdrawal of the 35 USC §102(a) rejections of claims 12-20 is respectfully requested.

Additionally, claims 12-20 include further features that are not anticipated by Nerurkar. In rejecting respective ones of claims 12-20, the Action rejects these claims on a similar rationale used to reject claims 2-10. For the reasons already

discussed above with respect to claims 2-10, Applicant respectfully submits that Nerurkar does not anticipate these additional features of claims 12-20.

Accordingly, for these additional reasons, withdrawal of the 35 USC §102(a) rejections of claims 12-20 is respectfully requested.

Claim 21 recites: "A device comprising: a memory comprising computer-executable instructions for providing application security threat-modeling", "a processor that is operatively coupled to the memory, the processor being configured to fetch and execute the computer-executable instructions from the memory, the computer-executable instructions comprising instructions for: defining a plurality of model components to represent respective elements of an application, each model component comprising a respective set of potential security threats", "interconnecting the model components to form a logical model of the application", and "analyzing one or more of the potential security threats in terms of the model components in the logical model."

The Action rejects claim 21 on the same rationale used to reject claim 1. In view of this, Applicant respectfully submits that for the same reasons discussed above with respect claim 1, Nerurkar does not anticipate claim 21.

Accordingly, withdrawal of the 35 USC §102(a) rejection of claim 21 is respectfully requested.

Claims 22-30 depend from claim 21 and are not anticipated by Nerurkar solely in view of these respective dependencies. For this reason alone, withdrawal of the 35 USC §102(a) rejections of claims 22-30 is respectfully requested.

Additionally, claims 22-30 include further features that are not anticipated by Nerurkar. In rejecting respective ones of claims 22-30, the Action rejects these claims on a similar rationale used to reject claims 2-10. For the reasons already

discussed above with respect to claims 2-10, Applicant respectfully submits that Nerurkar does not anticipate these additional features of claims 22-30.

Accordingly, for these additional reasons, withdrawal of the 35 USC §102(a) rejections of claims 22-30 is respectfully requested.

Claim 31 recites: "A user interface for application security threat-modeling, the user interface comprising: means for displaying and interconnecting a plurality of model components to design a logical model of an application, at least a subset of the model components comprising a corresponding set of potential security threat characteristics", "means for specifying a component of the model components", and "means for addressing one or more of the potential security threats in terms of the model components in the logical model." The Action rejects claim 31 on the same rationale used to reject claim 1. Applicant respectfully disagrees.

While a means-plus-function limitation may appear to include all means capable of achieving the desired function, the statute requires that it be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof. More particularly, to interpret means-plus-function claims, one must resort to the last paragraph of 35 USC §112. The statute expressly states that the patentee is entitled to a claim covering equivalents as well as a specified "structure, material or act." In view of this, and for the reasons already discussed above with respect claim 1, Nerurkar does not anticipate claim 31.

In another example of why the mean-plus-function features of claim 31 are patentably distinguished from Nerurkar, consider that Nerurkar does not explicitly or inherently describe, a computer system to implement security threat-modeling

and analysis software used to design security into an application (e.g., see Fig. 6 of Applicants specification and corresponding description, which provide "structure, material or act" and equivalents thereof, to which the coverage of claim 31 is clearly entitled). Instead Nerurkar describes a step-by-step method for a human being to manually model and analyze security threats.

For these additional reasons, the Action has not presented a prima facie case of anticipation of claim 31, and withdrawal of the 35 USC §102(a) rejection of claim 31 is respectfully requested.

Claims 32-36 depend from claim 31 and are not anticipated by Nerurkar solely in view of these respective dependencies. For this reason alone, withdrawal of the 35 USC §102(a) rejections of claims 32-36 is respectfully requested.

Additionally, claims 32 and 33 include further features that are not anticipated by Nerurkar. In rejecting claims 32 and 33, the Action rejects these claims on a similar rationale used to reject claims 2 and 3. For the reasons already discussed above with respect to claims 2 and 3, Applicant respectfully submits that Nerurkar does not anticipate these additional features of claims 32-33.

Accordingly, for these additional reasons, withdrawal of the 35 USC §102(a) rejections of claims 32-33 is respectfully requested.

Conclusion

Claims 1-36 are in condition for allowance, and action to that end is respectfully requested. Should any issue remain that prevents allowance of the application, the Office is encouraged to contact the undersigned prior or issuance of a subsequent Office Action.

Respectfully Submitted,

Dated: 8/15/05 By: Brian Hart

Brian G. Hart
Reg. No. 44, 421
(509) 324-9256